



Federated Identity

**Michelle Dennedy
Chief Privacy Officer
Sun Microsystems, Inc.**



Concept of Identity

Identity can be defined as "a set of information by which one person is definitively distinguished."

People are now creating online identities specific to the organizations with which they interact. These can be considered "personas".

Context matters.

Some Dennedy persona elements...

- I am a mommy & a wife
- I work for Sun Microsystems, Inc.
- I am interested in identity, privacy, policy & cultural issues
- I am a sucker for sappy country music
- I hate to fly
- I listen to recorded books (Snow Crash by Neal Stephenson right now)

What's the difference...?

In real life:

- Information disclosure is often deliberate
- We tend to know when we are doing it, and to whom
- It usually generates feedback
- We adjust our behaviour accordingly over time
- Disclosure is contextual
- There is "friction" which acts as a brake on disclosure

Online:

- We may not be conscious that we are disclosing information, or to whom
- 'Behavior' data is much easier to collect
- We may get little or no feedback
- Bad behavior seems to have no consequences!
- "Frictionless" transactions may mean frictionless disclosure

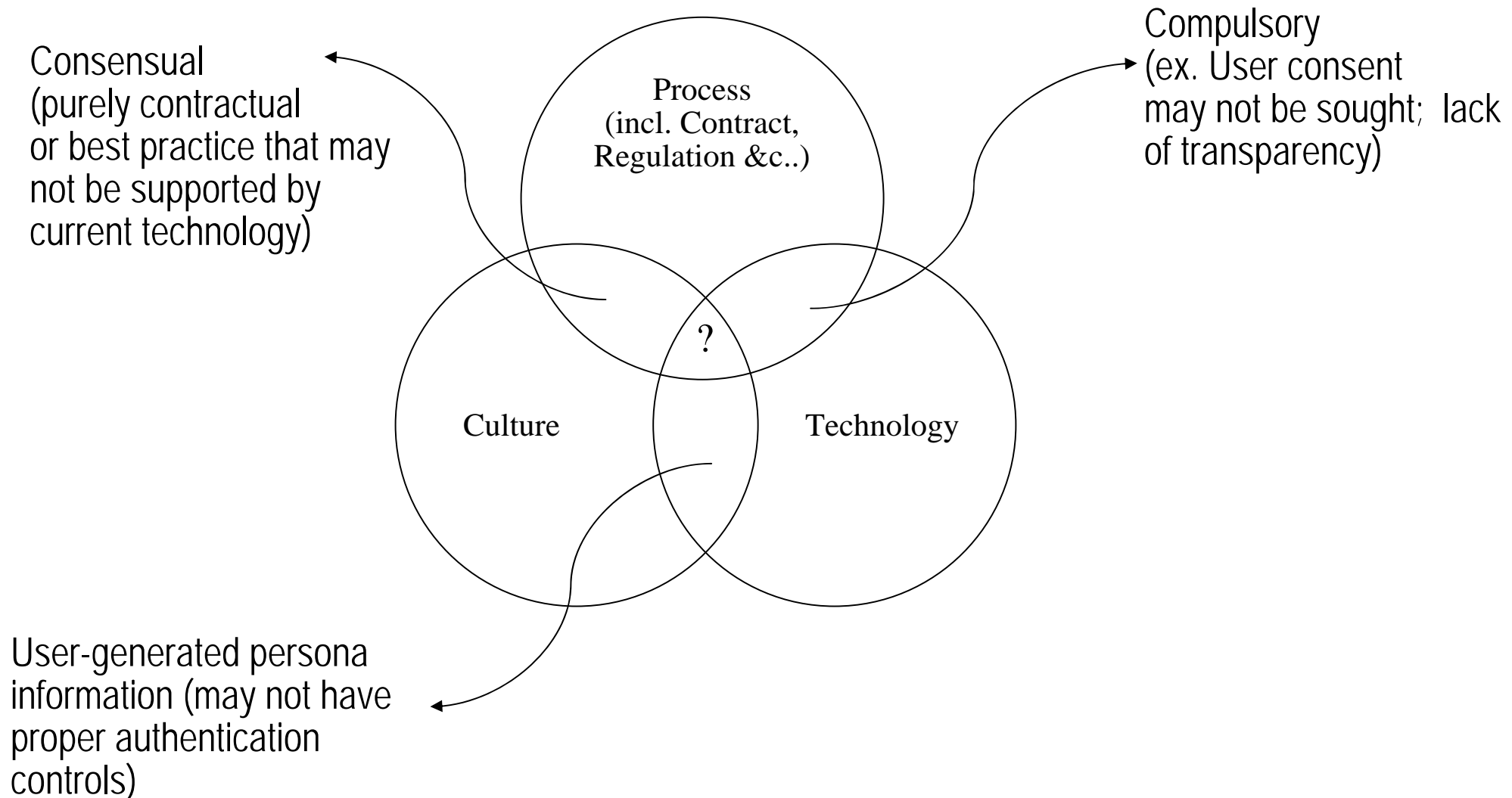
The Challenge We Face

- The online world does not always look like nor behave like the real world;
- The online world may presents us with metaphors to help explain these differences, but not easy solutions to resolve them;
- We therefore frequently base our behavior on a flawed perception of risk.

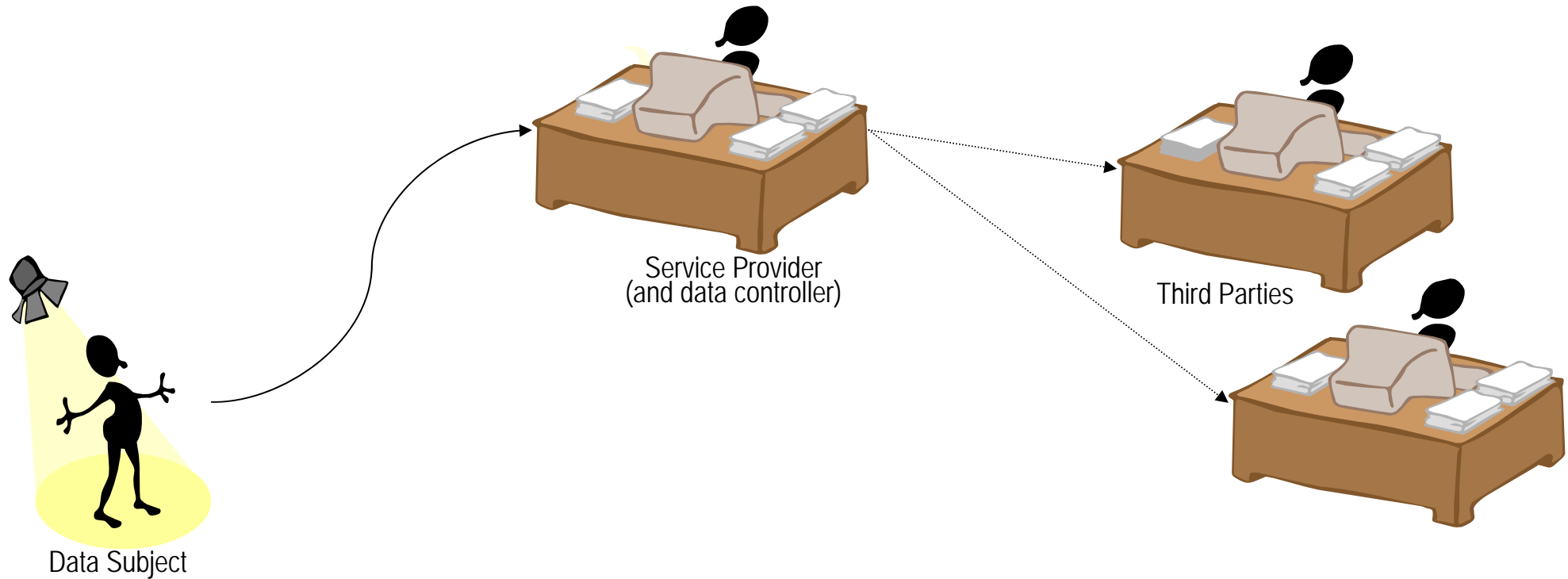


In other words, we could be surfing naked and not even know it. Brrr.

Is there a privacy 'sweet spot'?



Who is in control here?



Contractual Protection, Privacy Policy/Preferences

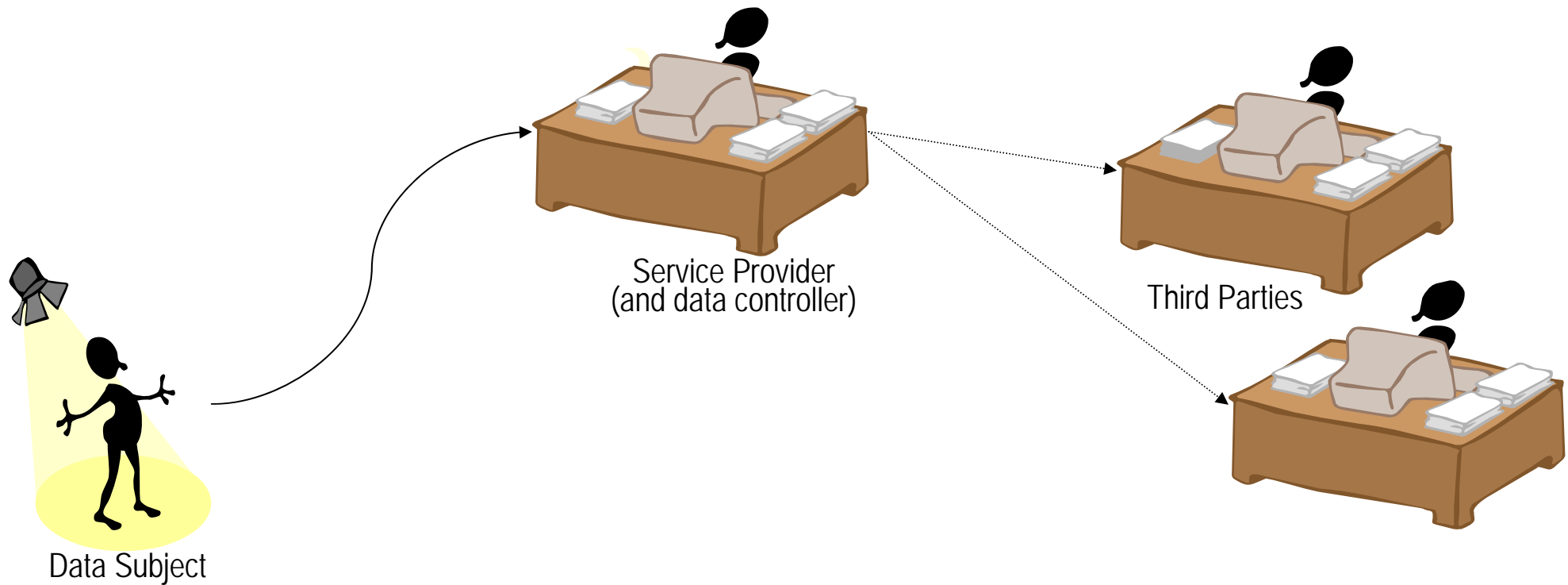
Non-technical Protection - auditable?

Technical Protection, Policy Enforcement

Technical Protection - available?

Whether technically or contractually, policy may not be translated equally across organizations

Is a technical approach viable?



Privacy Preference Expression

Privacy Preference Enforcement

Purpose of Use (or Disclosure)

Purpose of Collection

Purpose for Use, Purpose of Collection, Protection measures & Destruction schedules must also be consistent, but sometimes are not...

Federated Identity

Identity federation allows the user to link, connect, or bind personas that have been created by a person for multiple service providers.

Linked personas, may be referred to as a *federated identity*.

This can allow a user to log in to one service provider site and click through to an affiliated service provider with certain authentication characteristics intact.

Federation Goals: Project Liberty

- Serve as open standards for federated identity management and web services.
- Support and promote permission-based sharing of personal identity attributes.
- Provide a standard for Simple Sign On.
- Create a platform for authorization for multiple providers.
- Create an open network identity infrastructure that supports all current and emerging browsers.
- Enable consumers to protect and manage their persona information on the Network.

Some Advantages of a Federated Approach

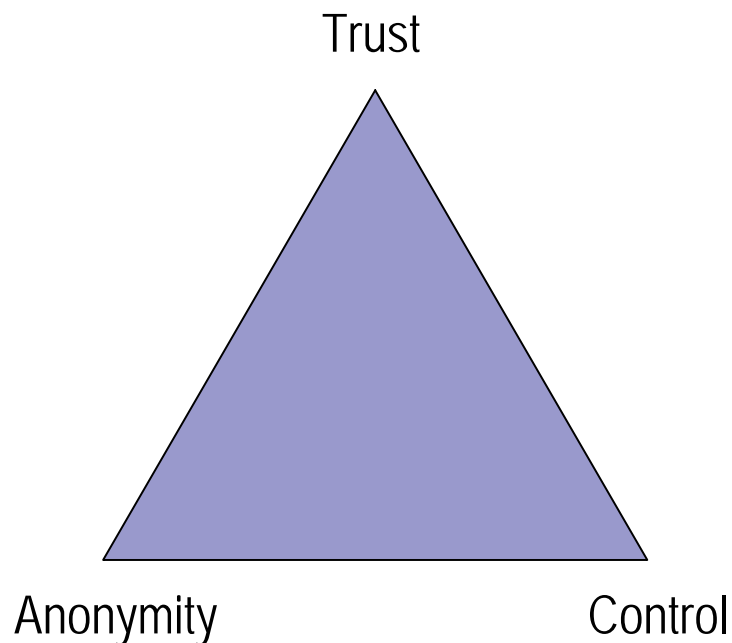
- Experience shows that multi-party federation only works if proper attention is also paid to the non-technical framework.
- Permission-based exchange of user attributes (notice & consent) is facilitated.
- Reduced movement of PII data from place to place.
- The federated model provides a much better online analogue for 'real-world' trust relationships.

But...

- More investigation is perhaps needed to ensure 'policy persistence' across & within organizations.

Some considerations ...

- Consent
- Roles
- Personas



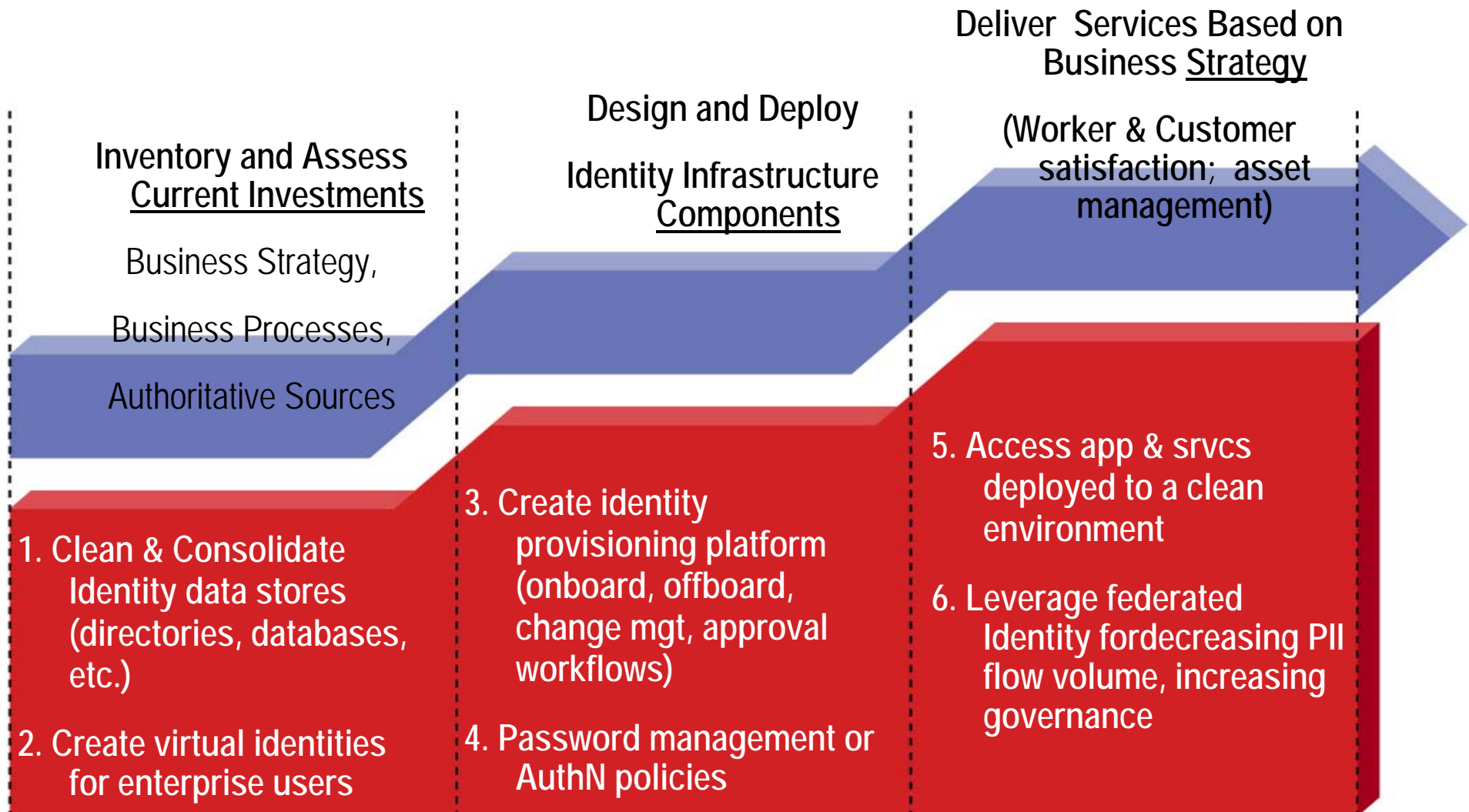
- Most instances of identity theft happen when the subject's data is outside their control
- User 'assertions' are a key part of online interaction
- What happens when you remove someone's ability to have secrets?
- Just like identity theft, privacy requires a holistic approach:
 - Legislation, Regulation, Best Practice, Technology, Process and User Behavior are all factors



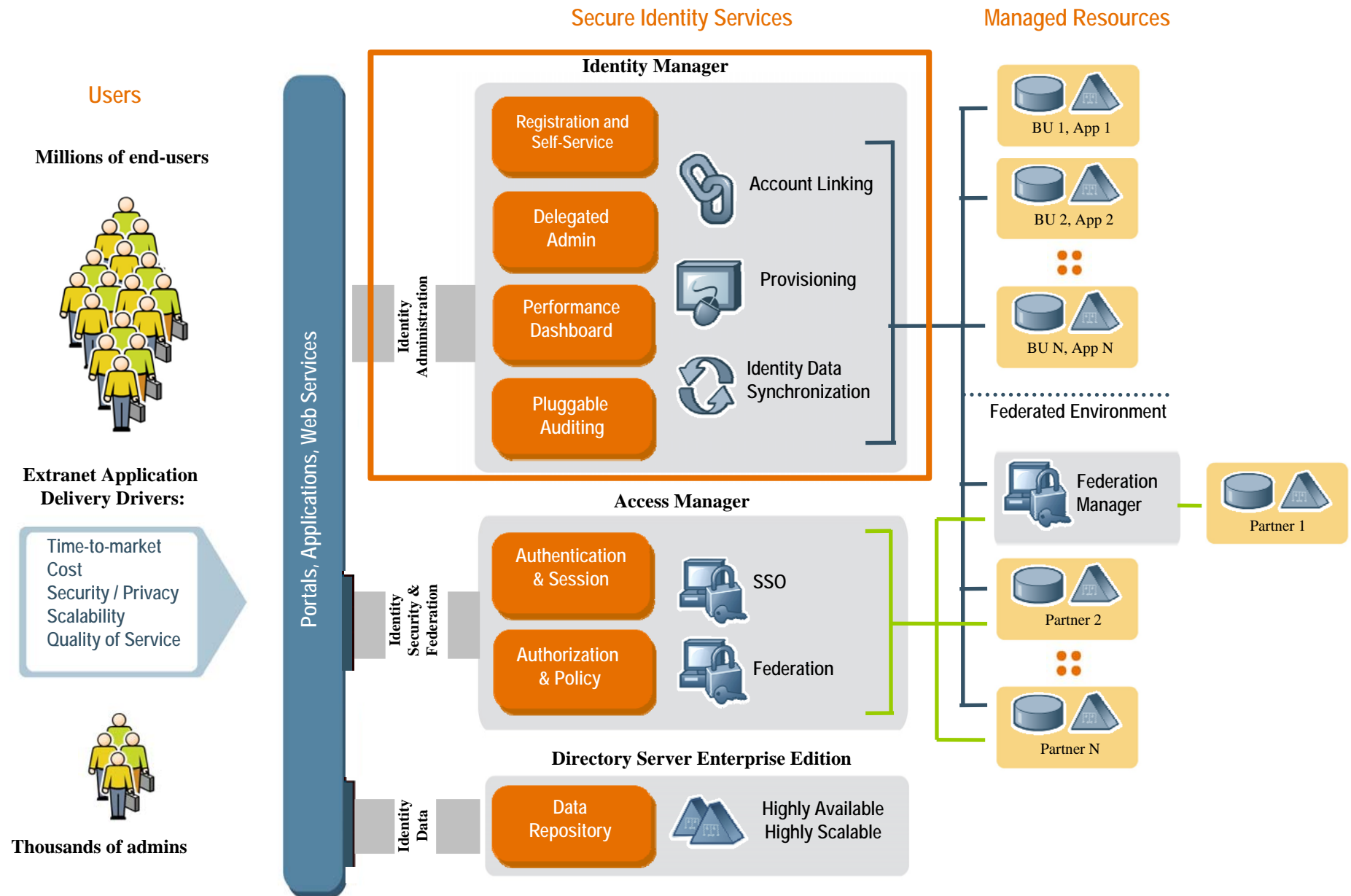
michelle.denney@sun.com
blogs.sun.com/suncpo

Do You Have an Identity Strategy In Place?

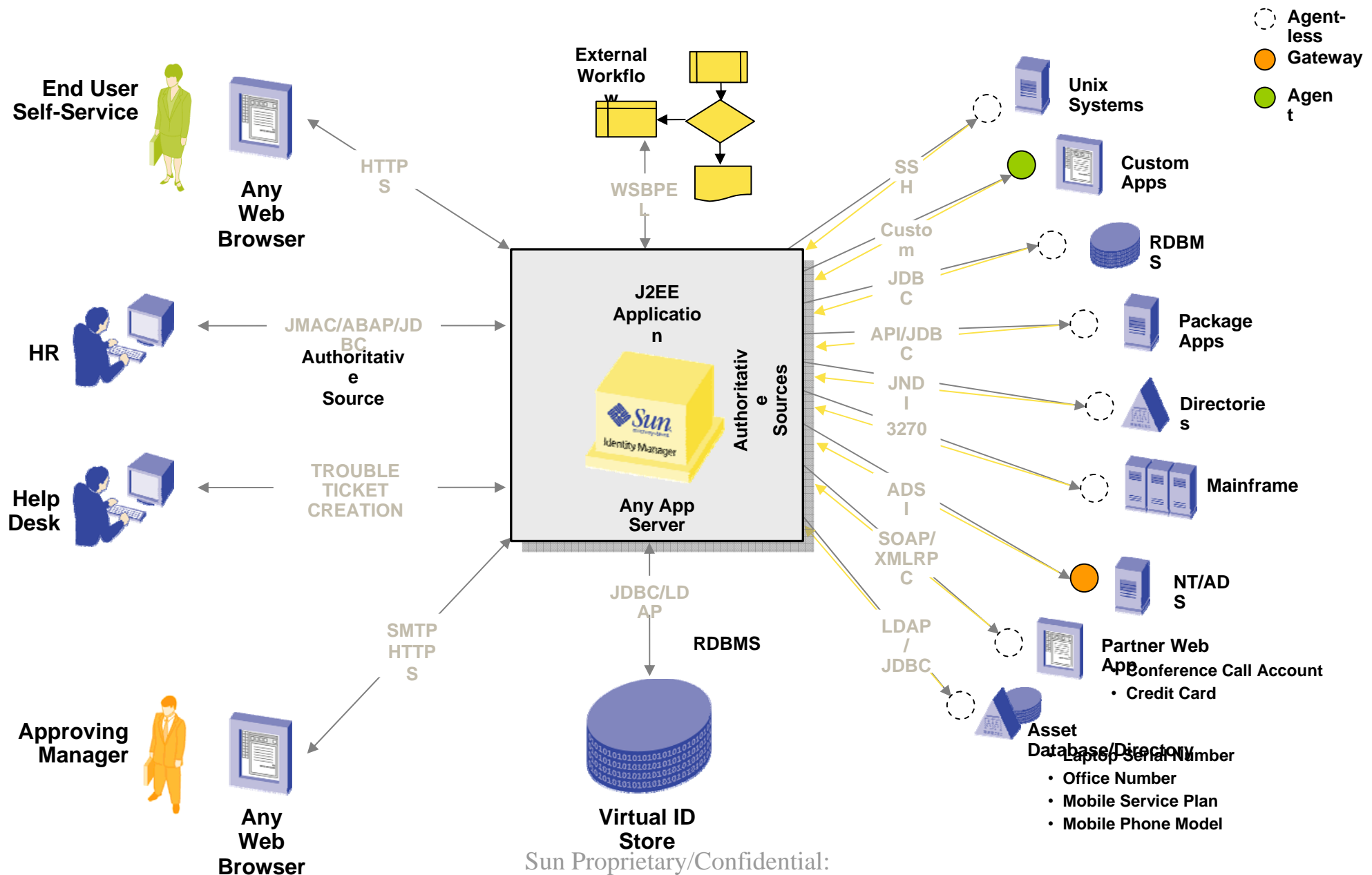
How To Start Getting your Identity Infrastructure in Order



Extranet Identity with Sun IDm

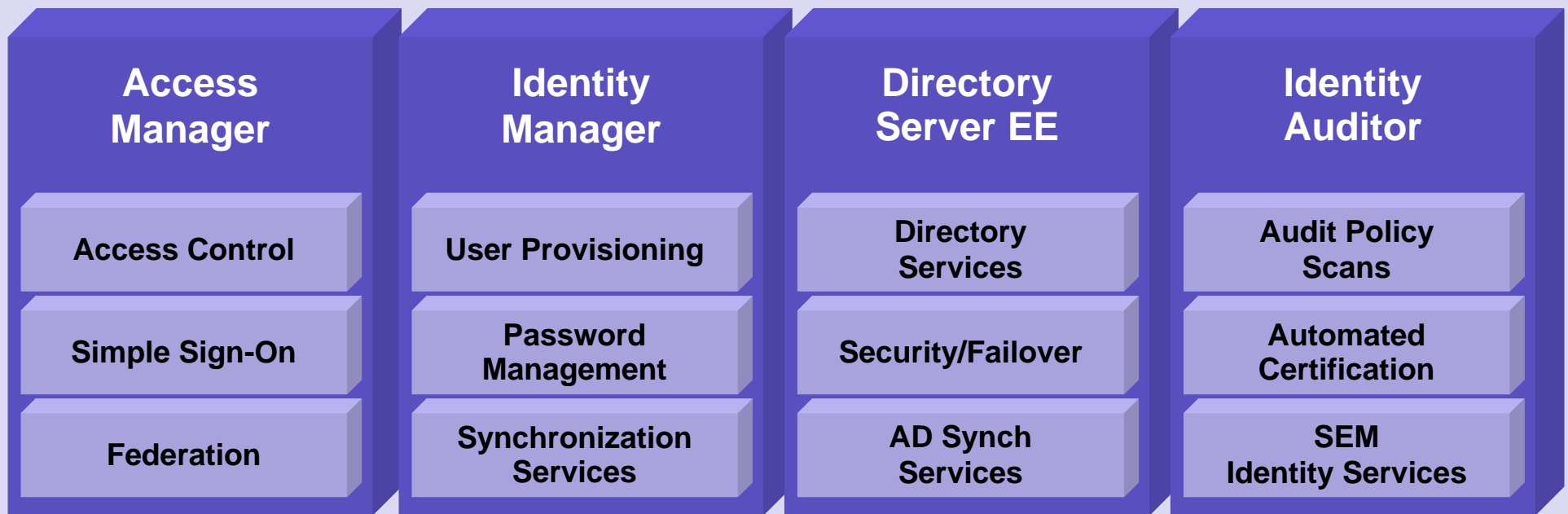


Identity Manager Overview Topology



Sun Identity Suite

Web-Based Administration



Reporting